Configurazione di LDAP in Intersight Virtual Appliance

Sommario

Introduzione

In questo documento viene descritto il processo di configurazione dell'autenticazione LDAP in un'appliance PVA (Intersight Private Virtual Appliance).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Protocollo LDAP (Lightweight Directory Access Protocol).
- Intersight Private Virtual Appliance.
- Server DNS (Domain Name Server).

Componenti usati

- Intersight Private Virtual Appliance.
- Microsoft Active Directory
- Server DNS.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

LDAP è un protocollo utilizzato per accedere alle risorse da una directory attraverso la rete. In queste directory vengono memorizzate informazioni su utenti, organizzazioni e risorse. LDAP fornisce un modo standard per accedere e gestire le informazioni che possono essere utilizzate per i processi di autenticazione e autorizzazione.

In questo documento viene illustrato il processo di configurazione per aggiungere l'autenticazione remota tramite LDAP a un PVA di Intersight.

Configurazione

Configurazione delle impostazioni di base di LDAP

1. Selezionare Sistema > Impostazioni > AUTENTICAZIONE > LDAP/AD.
2. Fare clic su Configura LDAP.
3. Immettere le informazioni richieste. Prendere in considerazione i suggerimenti seguenti:
    1. Il valore Name (Nome) viene impostato in modo arbitrario e non influisce sulla configurazione.
    2. Per i valori BaseDN e BindDN, copiare e incollare i valori corrispondenti dalla configurazione di Active Directory (AD).
    3. Il valore predefinito per Attributo gruppo è member.

    > Nota: In altri strumenti di gestione UCS, ad esempio UCSM o CIMC, l'attributo Group è impostato su memberOf. In Intersight si consiglia di lasciarlo come membro.

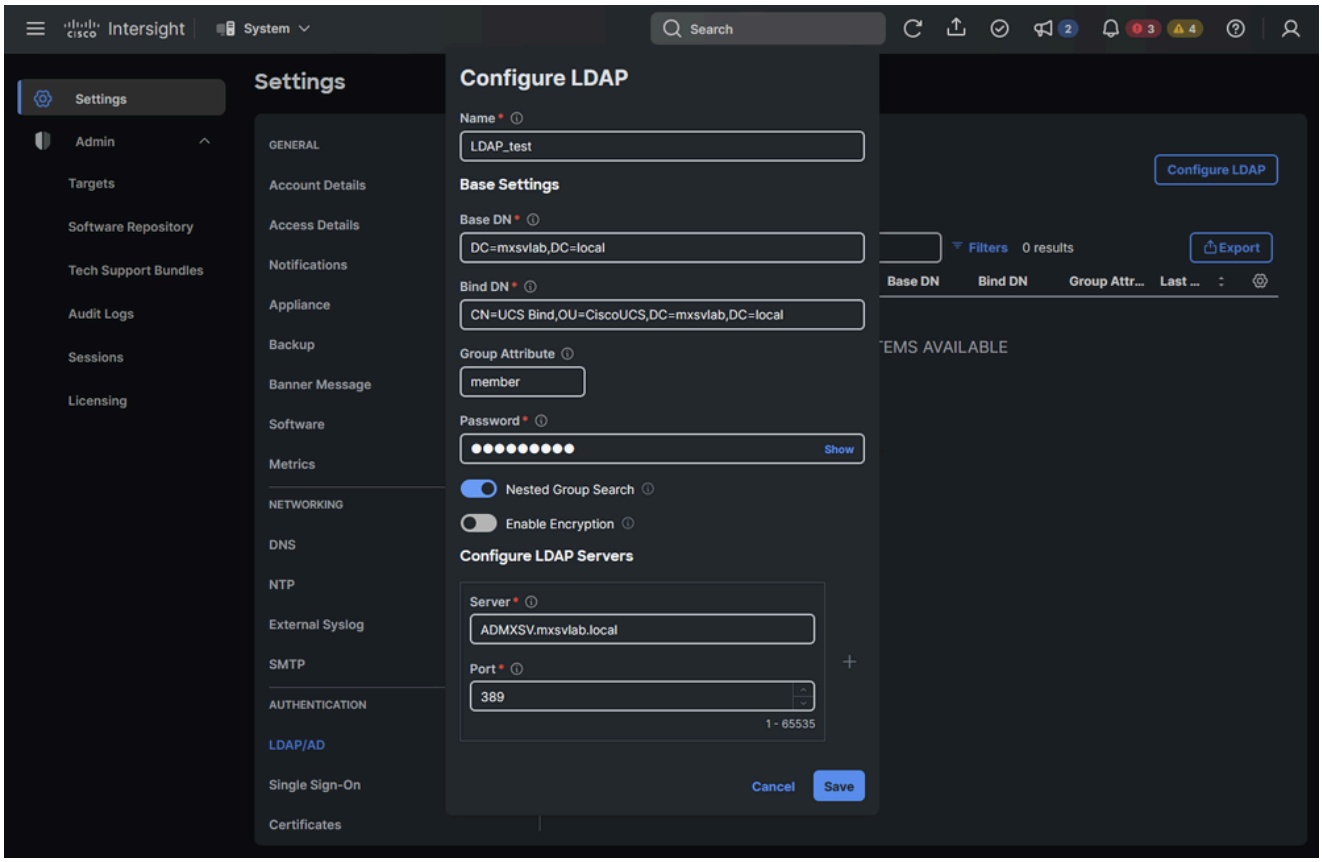
    4. Immettere la password per il provider LDAP.
    5. Abilitare Ricerca gruppo nidificato se si desidera consentire una ricerca ricorsiva in Active Directory per tutti i gruppi della radice e dei gruppi in essi contenuti.
    6. Lasciare disattivata l'opzione Abilita crittografia per una configurazione LDAP regolare. Se è necessario un LDAP sicuro, abilitarlo e assicurarsi di rivedere la sezione

Configurazione di LDAPS (LDAP sicuro) per i passaggi complementari da configurare.

4. Aggiungere la configurazione per un server LDAP:
    1. In Server introdurre l'indirizzo IP o il nome host del server LDAP.

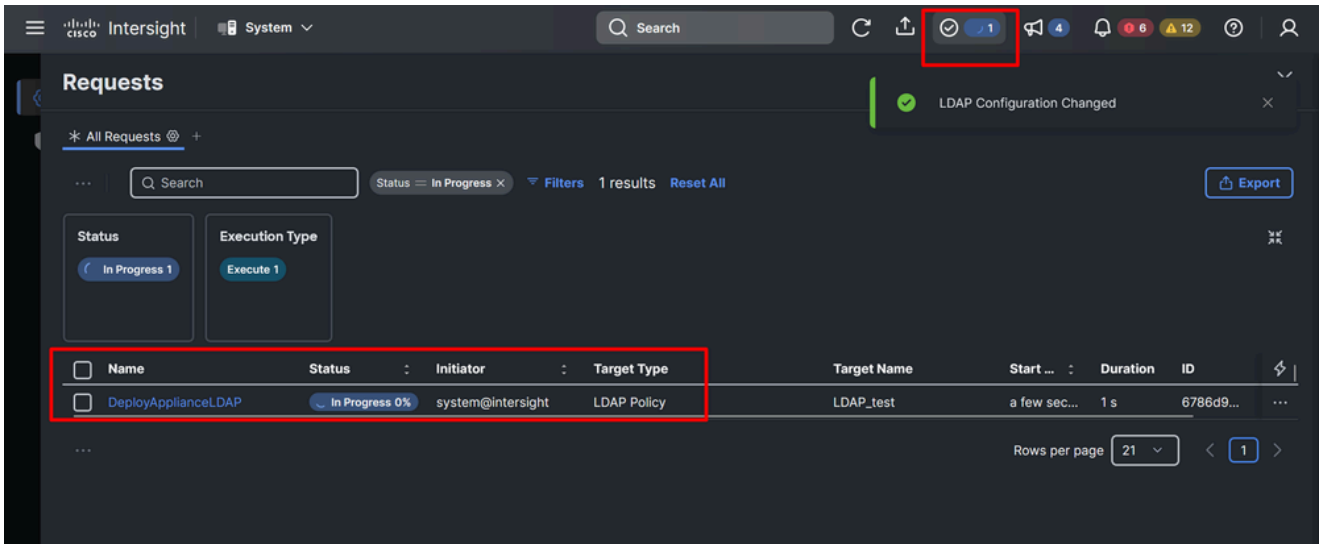
> ⚠ Attenzione: Se si utilizza hostname, verificare che il DNS sia in grado di eseguire correttamente il mapping di tale nome host.

    2. La porta predefinita e consigliata per LDAP è 389.
5. Fare clic su Save (Salva).



Esempio di configurazione per le impostazioni LDAP di base

6. Monitorare il flusso di lavoro DeployApplianceLDAP dalle richieste nella barra superiore.



Richiesta di distribuzione

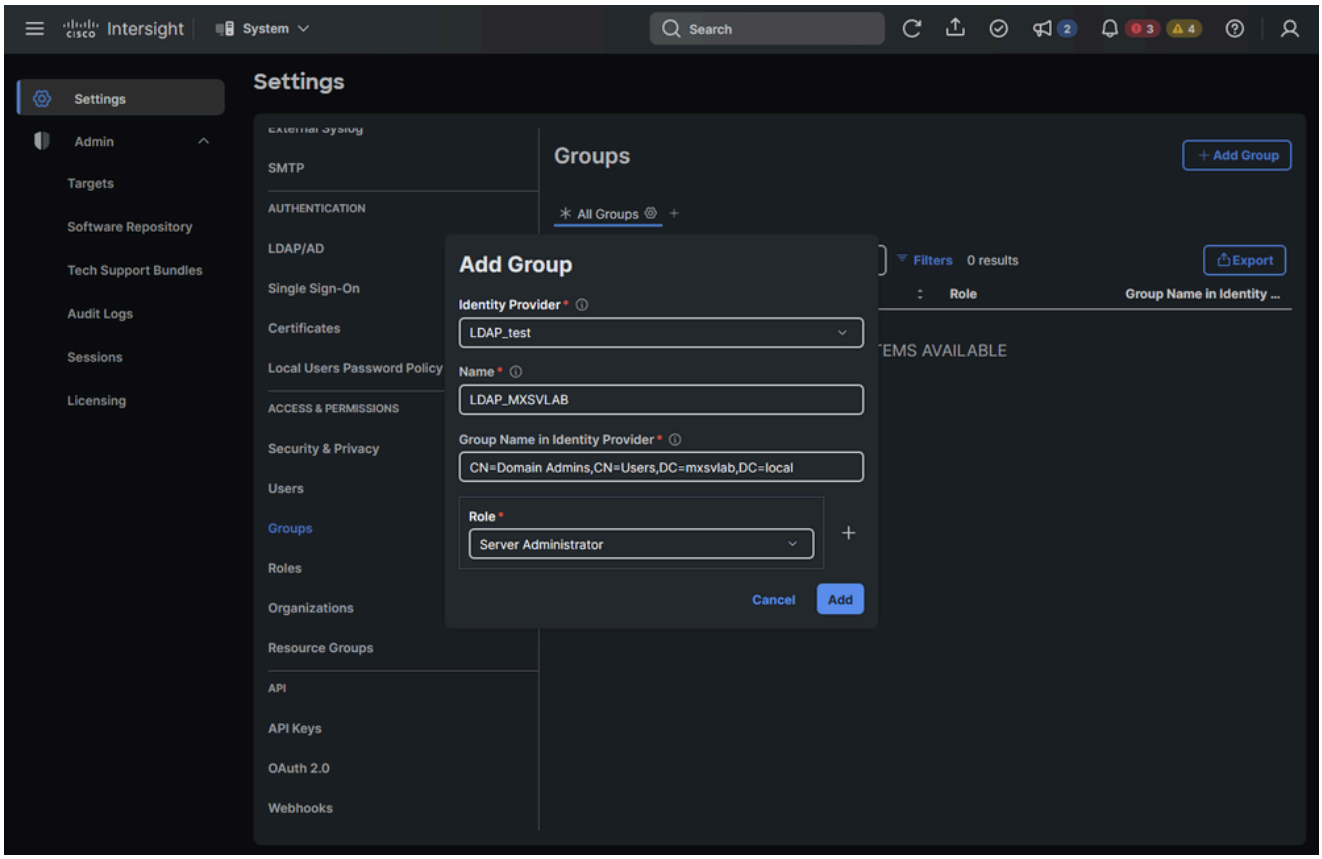
Configura utenti e gruppi

Una volta completato il flusso di lavoro DeployApplianceLDAP, è possibile configurare Gruppi o singoli utenti.

Se si decide di utilizzare Gruppi, l'autorizzazione viene fornita a tutti gli utenti che appartengono a tale Gruppo. Se si utilizzano singoli utenti, è necessario aggiungere ogni utente con il proprio ruolo di autorizzazione.

Configura gruppi

1. Selezionare Sistema > Impostazioni > ACCESSO E AUTORIZZAZIONI > Gruppi.
2. Fare clic su Aggiungi gruppo.
3. Selezionare il provider di identità. Si tratta del nome impostato nella sezione Configurazione delle impostazioni di base di LDAP.
4. Impostare un nome per il gruppo.
5. Immettere il valore per Nome gruppo in Provider di identità. Deve corrispondere alle configurazioni del gruppo nel server LDAP.
6. Selezionare il ruolo in base al livello di accesso che si desidera fornire agli utenti di questo gruppo. Vedere Ruoli e privilegi in Intersight.



Esempio di configurazione per un gruppo

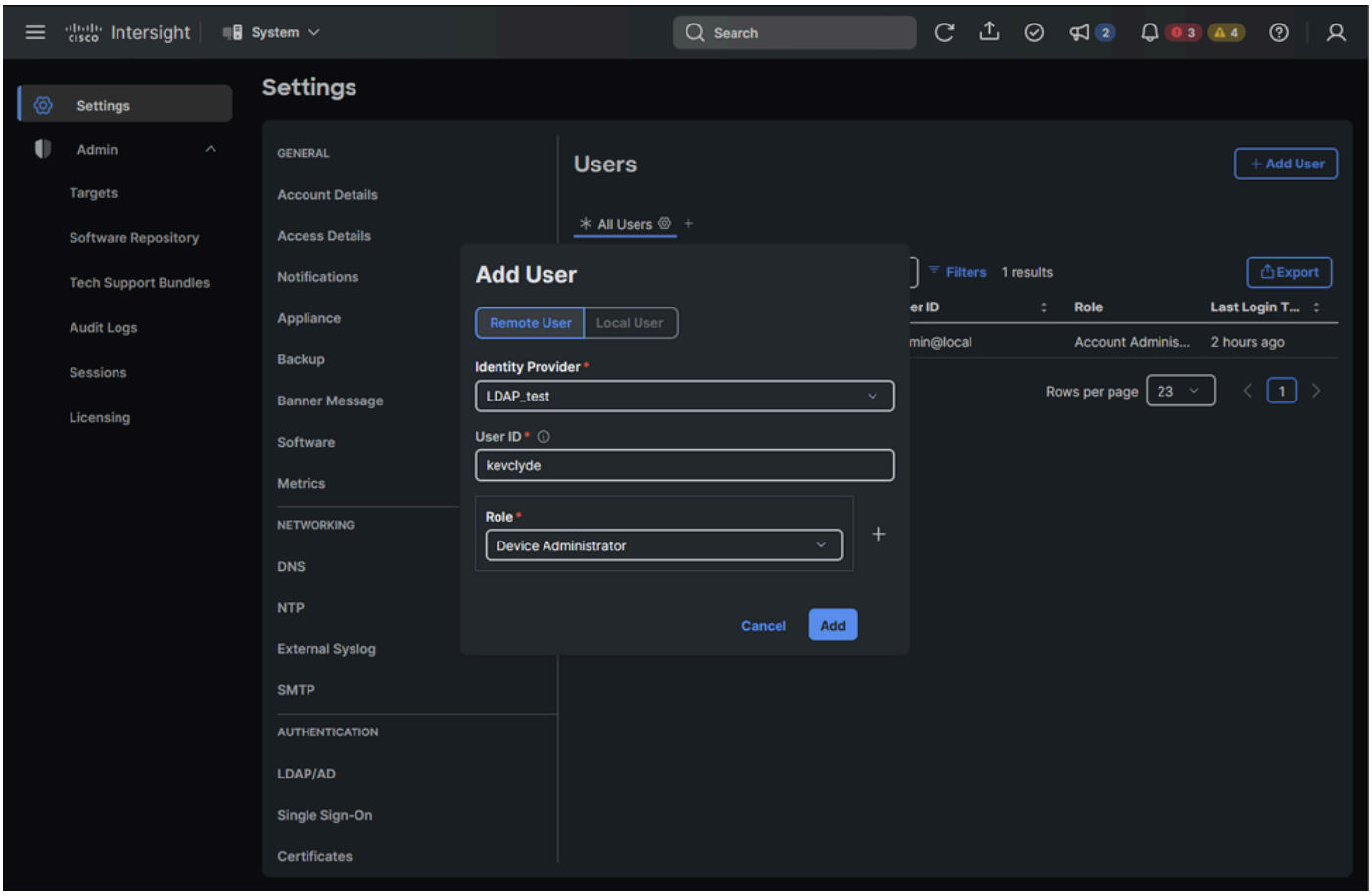
Configura utenti

Se si preferisce configurare singoli utenti anziché gruppi, attenersi alle seguenti istruzioni:

1. Selezionare Sistema > Impostazioni > ACCESSO E AUTORIZZAZIONI > Utenti.
2. Fare clic su Aggiungi utente.
3. Selezionare Utente remoto.
4. Selezionare il provider di identità. Si tratta del nome impostato nella sezione Configurazione delle impostazioni di base di LDAP.
5. Imposta un ID utente.

> Suggerimento: Per utilizzare il nome utente come metodo di accesso, copiare nel campo ID utente il valore configurato come sAMAccountName nel server LDAP. Se si desidera utilizzare l'e-mail, assicurarsi di impostare l'e-mail dell'utente nell'attributo mail nel server LDAP.

6. Selezionare il ruolo in base al livello di accesso che si desidera fornire all'utente. Vedere Ruoli e privilegi in Intersight.

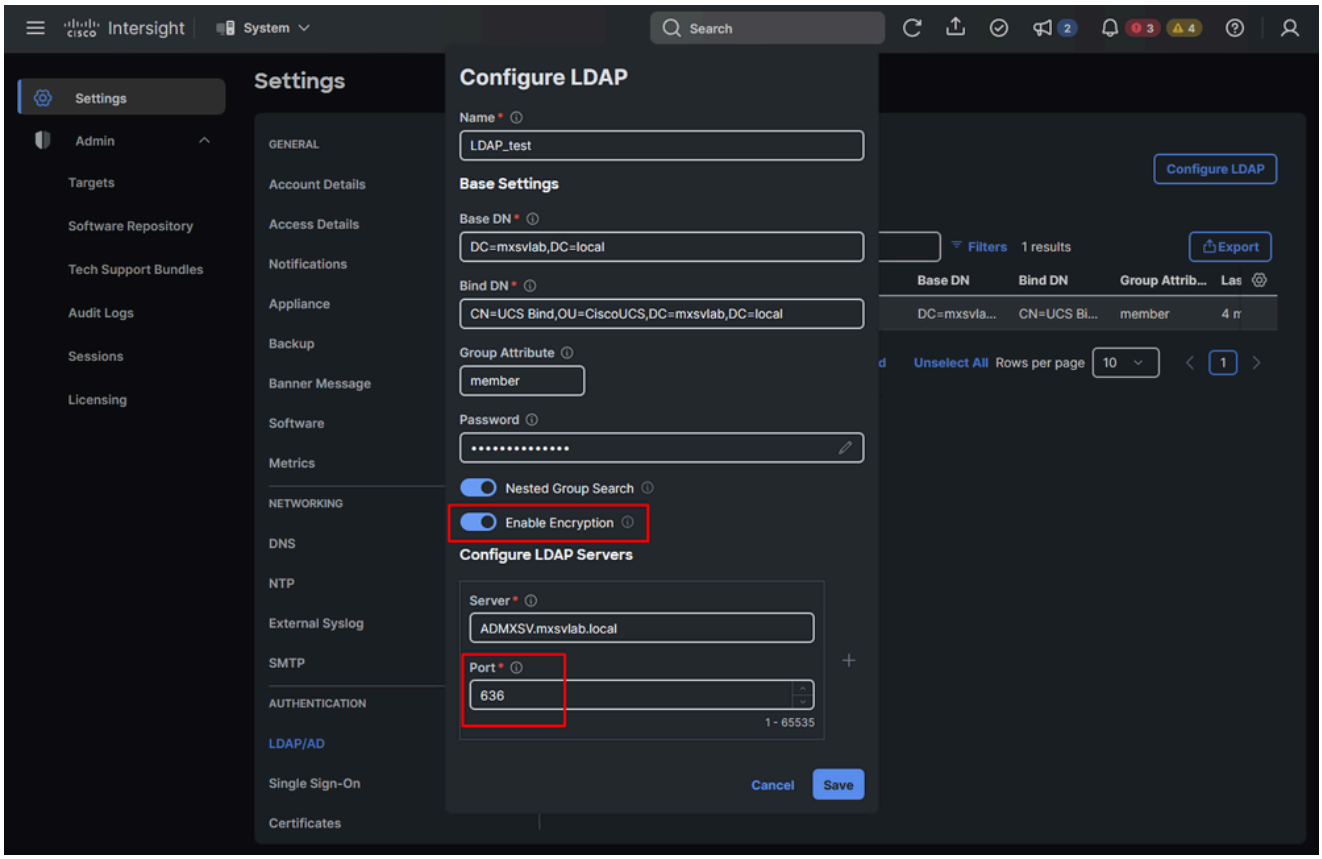


Esempio di configurazione per un utente

Configurazione di LDAPS (LDAP sicuro)

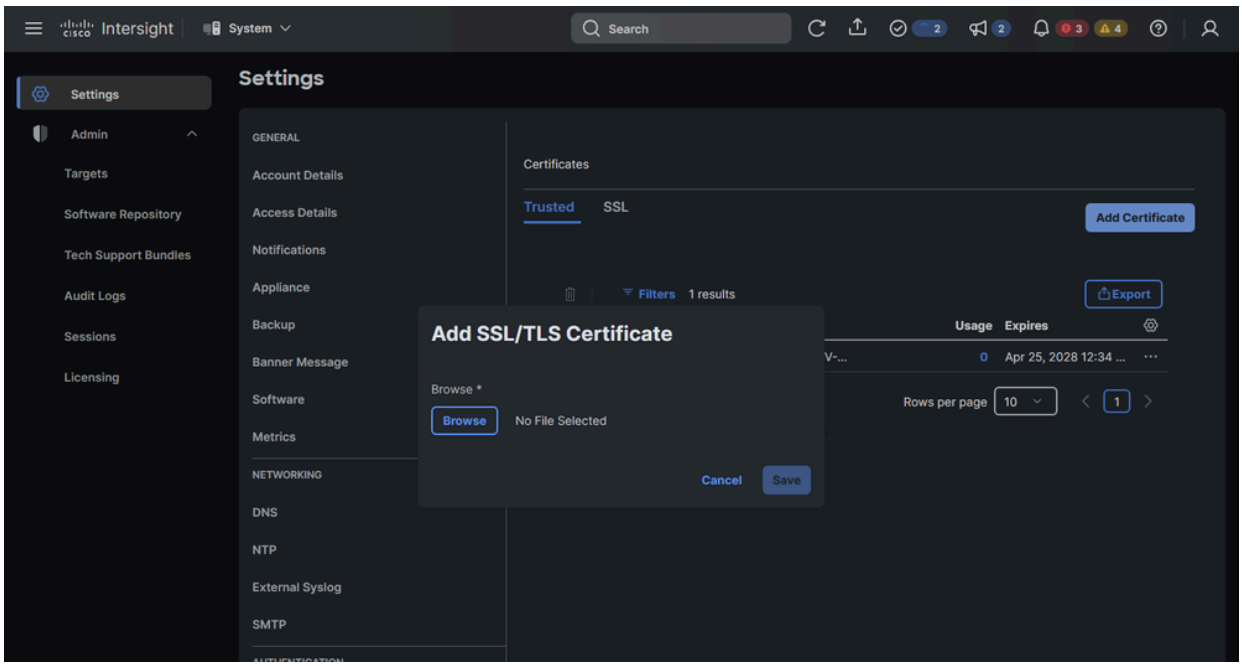
Se si desidera proteggere la comunicazione LDAP con la crittografia, è necessario disporre di un certificato firmato dalla CA. Accertarsi di applicare le seguenti modifiche alla configurazione:

1. Completare la procedura descritta in Configurazione delle impostazioni di base di LDAP assicurandosi di spostare il dispositivo di scorrimento Abilita crittografia a destra (fase 3.g).
2. Verificare che la porta utilizzata sia 636 o 3269 che sono le porte che supportano LDAPS (secure). Tutte le altre porte supportano LDAP su TLS.



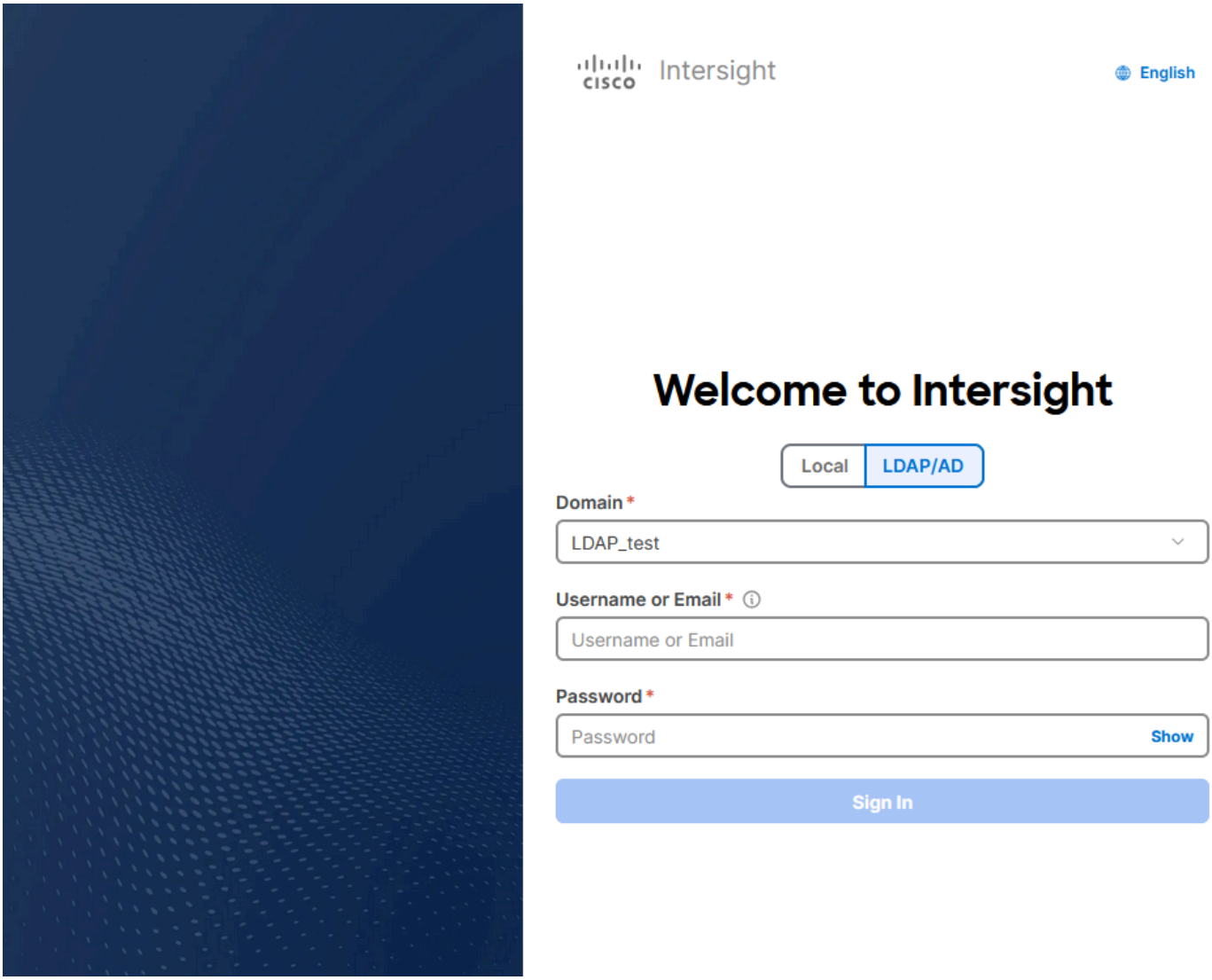
Modifiche alla configurazione per Secure LDAP

3. Salvare la configurazione e attendere il completamento del flusso di lavoro DeployApplianceLDAP.
4. Aggiungere un certificato con i passaggi seguenti:
    1. Selezionare Sistema > Impostazioni > AUTENTICAZIONE > Certificati > Attendibili.
    2. Fare clic su Aggiungi certificato.
    3. Fare clic su Sfoglia e selezionare un file .pem contenente il certificato rilasciato dalla CA.



Verifica

Nel browser passare all'URL di Intersight Virtual Appliance. Nella schermata viene ora visualizzata un'opzione per eseguire l'accesso con le credenziali LDAP:

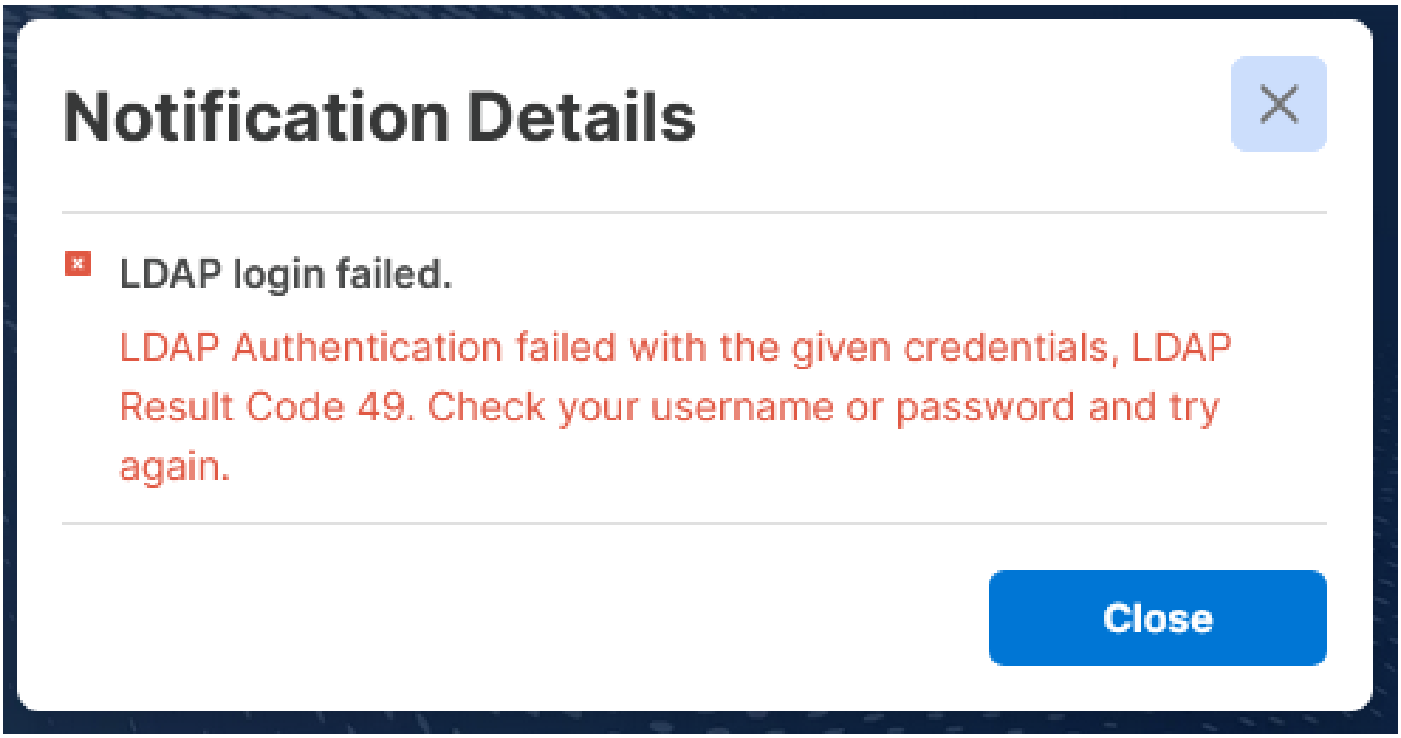


Configurazione LDAP abilitata dalla schermata di accesso

Risoluzione dei problemi

Se l'accesso non riesce, i messaggi di errore forniscono suggerimenti su ciò che potrebbe essere sbagliato.

Errore 1. Dettagli di accesso errati

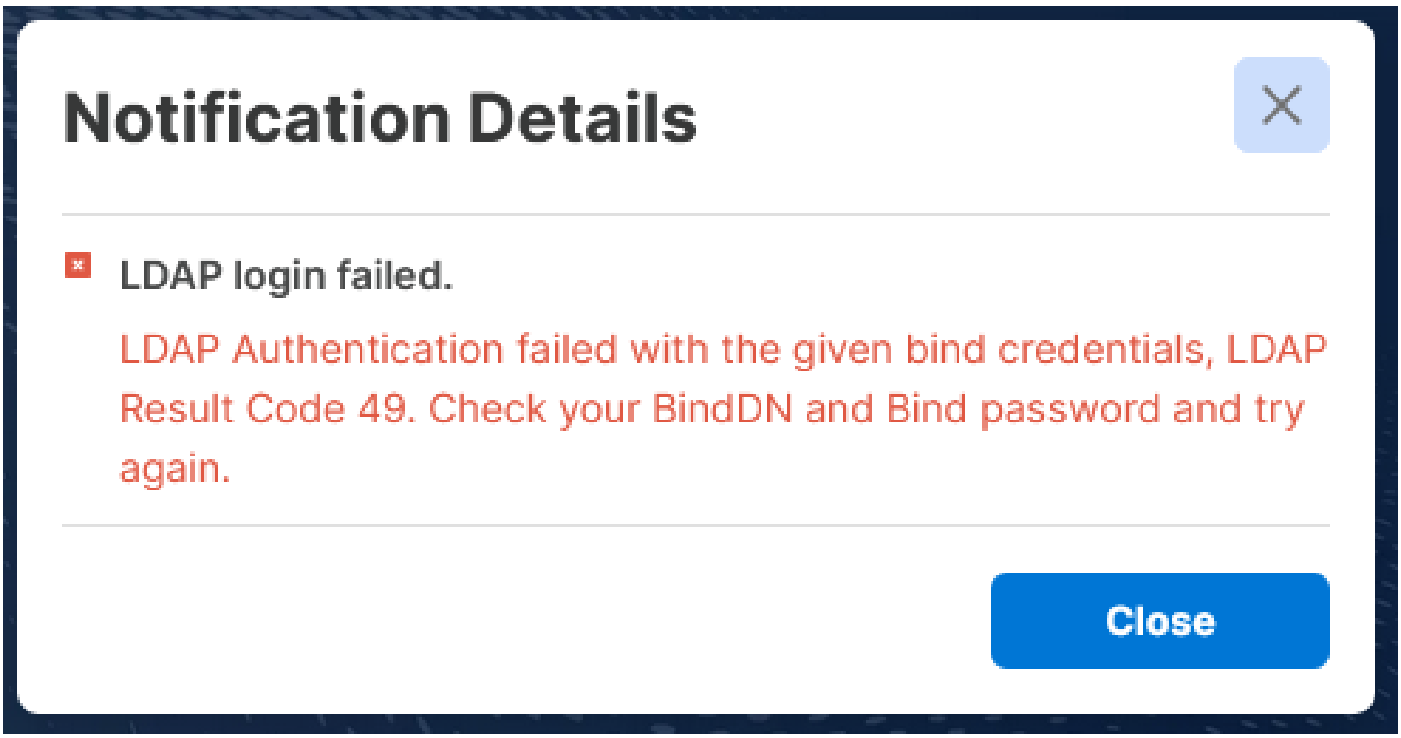


Messaggio di errore per password errata

Questo errore indica che i dati di accesso non sono corretti.

1. Verificare che il nome utente e la password siano corretti.

Errore 2. Dati di binding errati

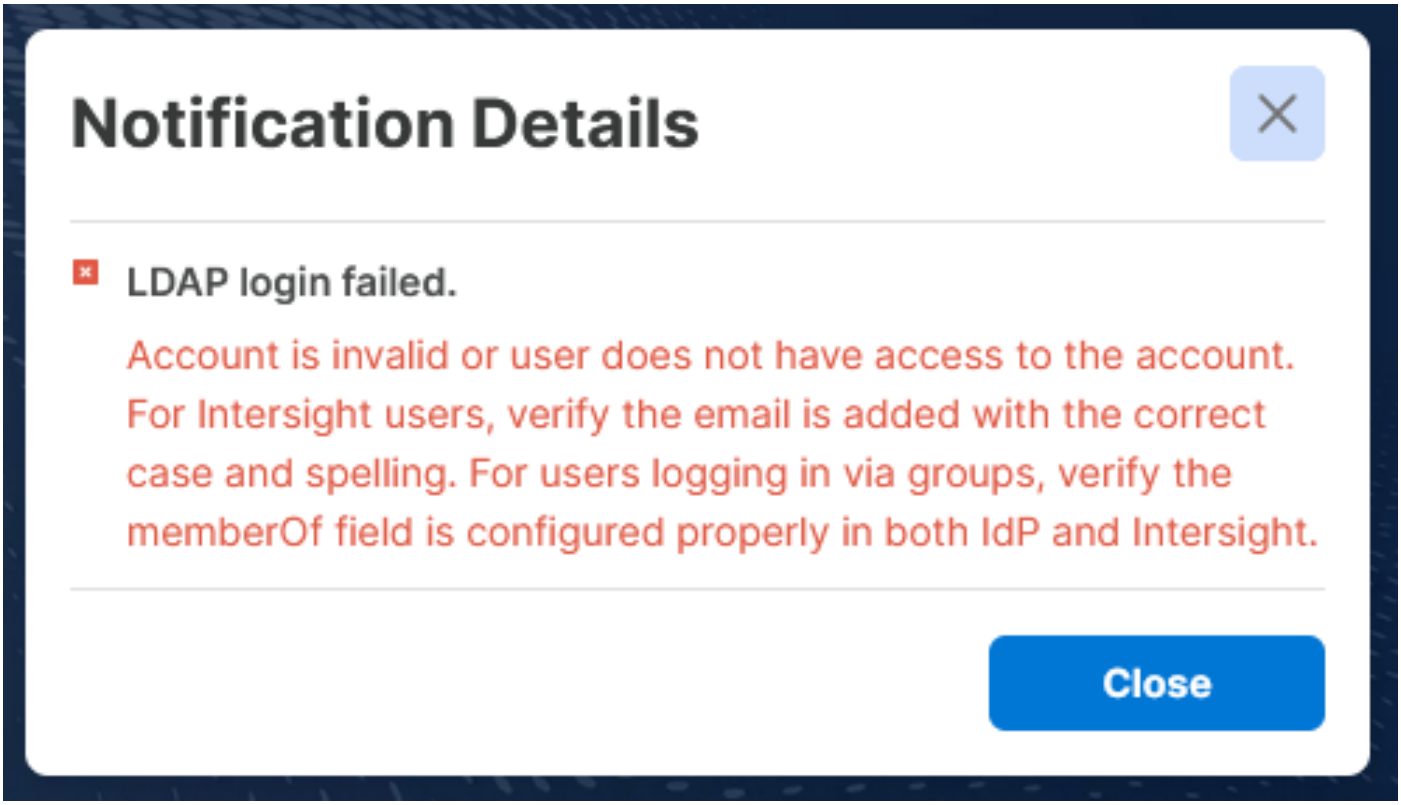


Messaggio di errore per dati di binding errati

Questo errore indica che i dati di associazione non sono corretti.

1. Verificare il valore BindDN.
2. Verificare la password di binding configurata nelle impostazioni LDAP.

Errore 3. Impossibile trovare l'utente

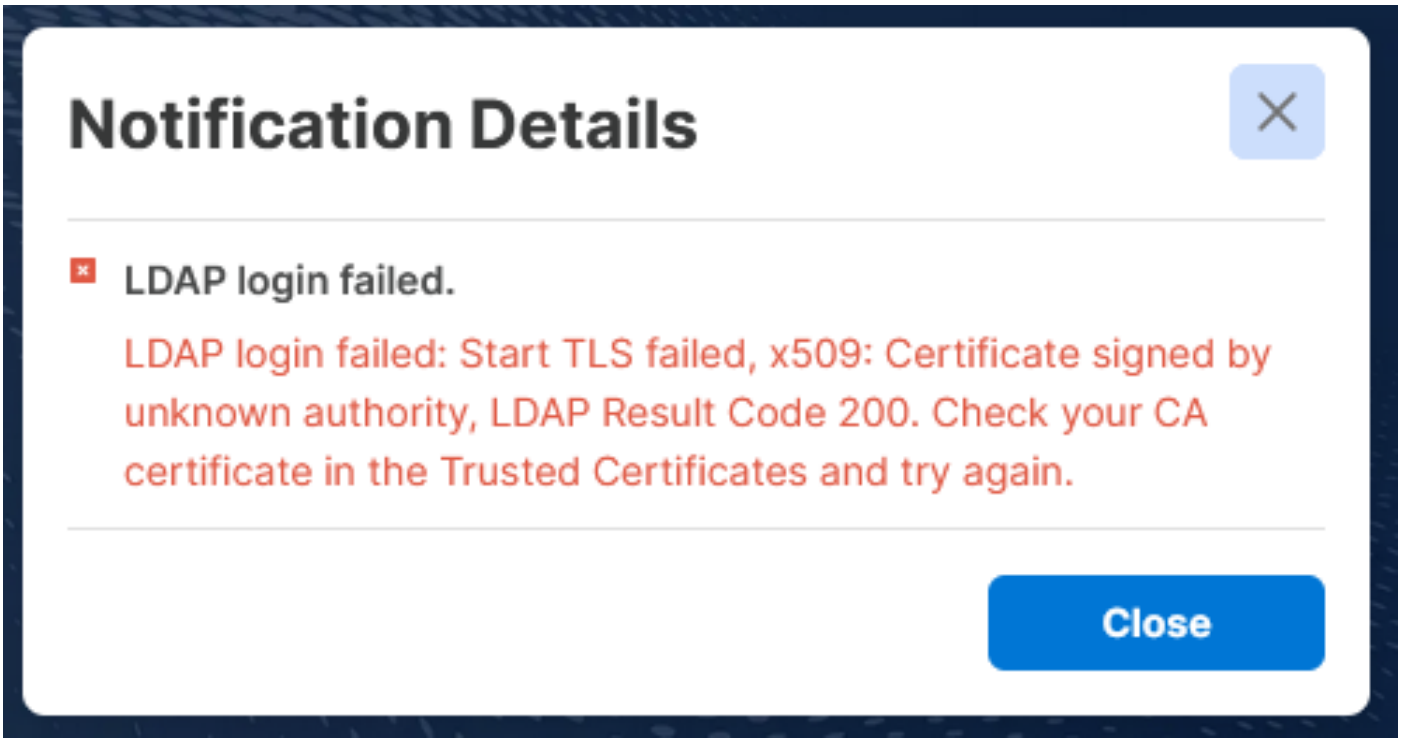


Messaggio di errore per utente non trovato

Questo viene attivato quando la ricerca nel server LDAP non restituisce alcun utente autorizzato. Verificare che le impostazioni successive siano corrette:

1. Selezionare BaseDN. I parametri utilizzati per la ricerca dell'utente sono errati.
2. Verificare che l'attributo Group sia impostato su member anziché su memberOf.
3. Verificare che il nome del gruppo nel provider di identità nella configurazione Gruppi sia corretto. Ciò si applica solo quando l'autorizzazione viene fornita tramite i gruppi.
4. Verificare che l'indirizzo di posta elettronica dell'utente sia impostato correttamente nel campo mail della configurazione di Active Directory per l'utente. Questa opzione si applica solo quando l'autorizzazione viene fornita a singoli utenti.

Errore 4. Certificato errato

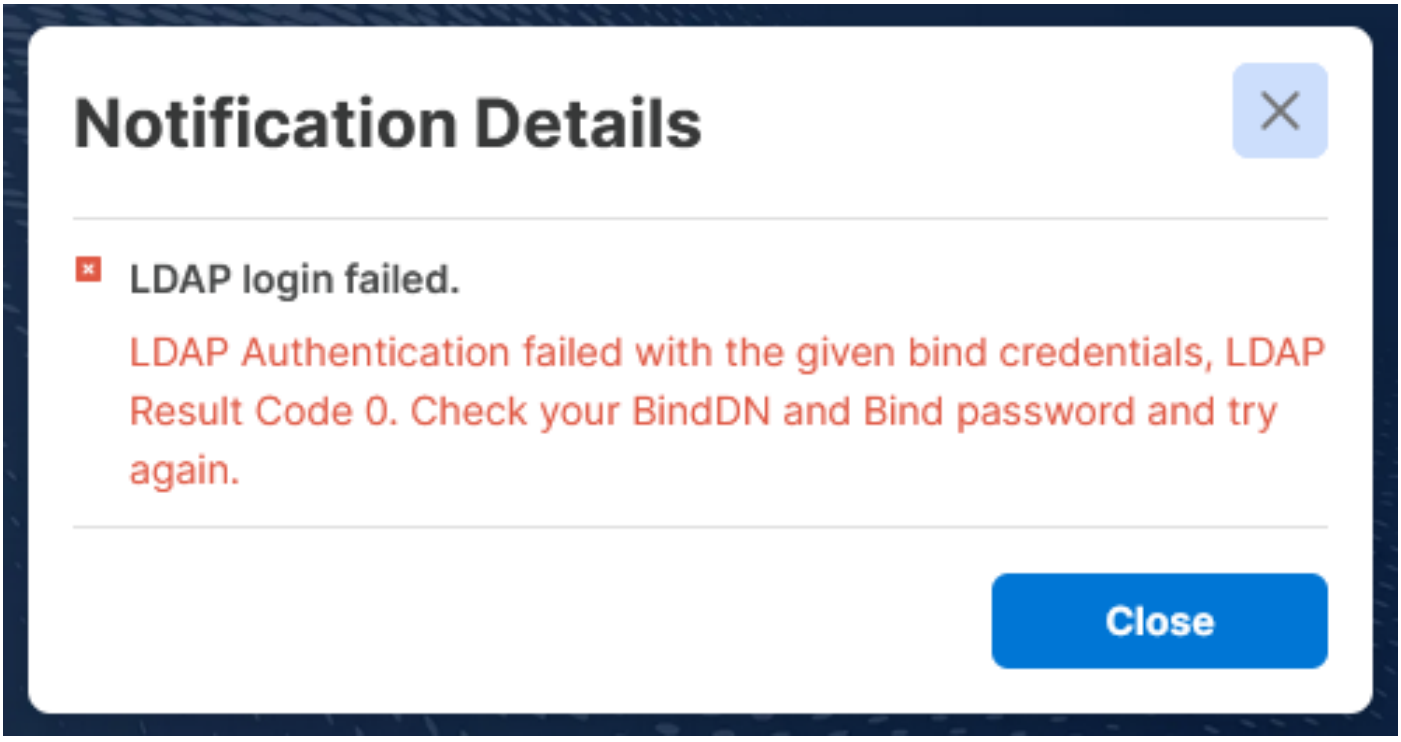


Messaggio di errore per certificato errato

Se LDAP crittografato è abilitato:

1. Verificare che il certificato sia configurato e che includa il certificato completo corretto.

Errore 5. L'opzione Enable Encryption (Abilita crittografia) viene utilizzata con una porta protetta

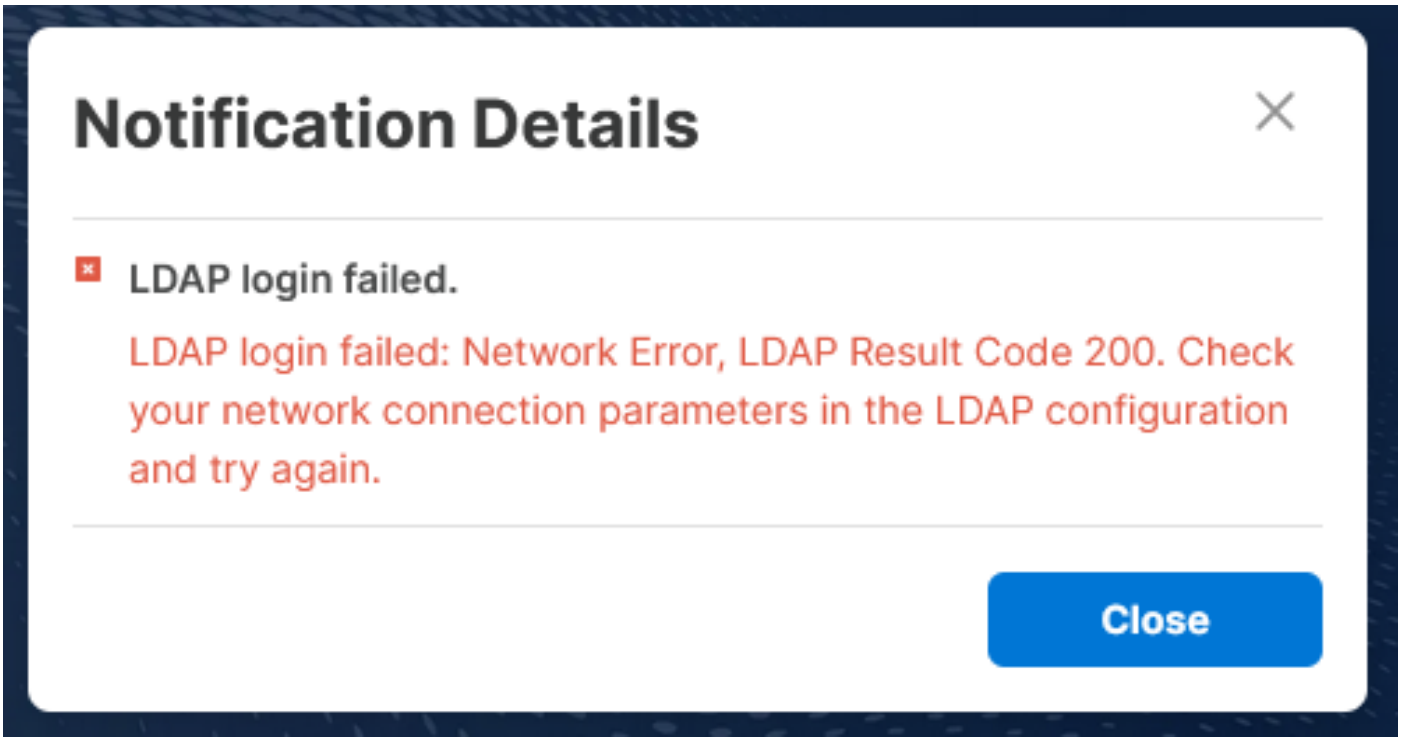


Messaggio di errore per l'abilitazione della crittografia disabilitata

Questo errore viene visualizzato quando l'opzione Enable Encryption non è abilitata ma è configurata una porta per il protocollo LDAP sicuro.

1. Se la crittografia non è abilitata, utilizzare la porta 389.

Errore 6. Parametri di connessione errati



Messaggio di errore per porta errata

Questo errore indica che non è stato possibile stabilire una connessione al server LDAP. Verificare:

1. Il server DNS deve risolvere il nome host del server LDAP nell'indirizzo IP corretto.
2. Intersight appliance è in grado di raggiungere il server LDAP.
3. Verificare che la porta 389 sia utilizzata per LDAP non crittografato, 636 o 3269 per LDAP sicuro (LDAPS) e qualsiasi altra porta per TLS (abilitare la crittografia e configurare un certificato).

Informazioni correlate

- Integrazione di Cisco Intersight Virtual Appliance con LDAP (video)
- Configurare le impostazioni LDAP in Intersight Appliance
- Ruoli e privilegi in Intersight
- Configurazione di esempio per LDAP in UCSM

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).